What is claimed is:

1. A method for authenticating a message recipient, said method comprising the steps of:

a) generating a password P;

b) sending said password P to said message recipient over a first, secure channel;

c) generating a first random number as a first initialization vector IV1;

d) generating H(IV1 | P) as an authentication key AK;

e) generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

f) generating a second random number as a second initialization vector IV2;

g) sending said vectors IV1 and IV2 to said message recipient over a second channel;

h) receiving a third random number as a third initialization vector IV3 and an authentication response AR from said recipient;

i) generating an authentication response key ARK as H(IV2 | IV3 | AS);

j) generating a decryption D(AR, ARK), where D is a symmetric decryption algorithm corresponding to E; and

k) authenticating said message recipient only if D(AR, ARK) = ACNST2, where ACNST2 is a second predetermined constant.

2. A method as described in claim 1 where:

a) steps a through f are carried out by a sender;

b) said sender sends said vector IV1 to said message recipient through a server, said server sending said vector IV1 together with said vector IV2 to said message recipient; and

c) said server receives said vector IV3 and said response AR from said recipient, and carries out steps i through k to authenticate said recipient.

3. A method as described in claim 1 where H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

4. A method as described in claim 3 where said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system.

5. A method as described in claim 4 where said encryption algorithm is an RC4 algorithm.

6. A method for sending an encrypted message, said method comprising the steps of:

a) generating a random number as an initialization vector IV4;

b) generating a private key PK as H(IV4 | P), where P is a password known to a message recipient;

c) generating an encryption ENC = E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm; and

d) sending (IV4, ENC) to said message recipient.

7. A method as described in claim 6 comprising the further step of receiving authentication of said message recipient prior to sending (IV4, ENC).

8. A method as described in claim 7 where said message recipient is authenticated by the steps of:

a) generating a password P;

b) sending said password P to said message recipient over a first, secure channel;

c) generating a first random number as a first initialization vector IV1;

d) generating H(IV1 | P) as an authentication key AK;

e) generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

f) generating a second random number as a second initialization vector IV2;

g) sending said vectors IV1 and IV2 to said message recipient over a second channel;

h) receiving a third random number as a third initialization vector IV3 and an authentication response AR from said recipient over said second channel;

i) generating an authentication response key ARK as H(IV2 | IV3 | AS);

j) generating a decryption D(AR, ARK), where D is a symmetric decryption algorithm corresponding to E; and

k) authenticating said message recipient only if D(AR, ARK) = ACNST2, where ACNST2 is a second predetermined constant.

9. A method as described in claim 8 where:

a) steps a through f are carried out by a sender;

b) said sender sends said vectors IV1 and IV2 to said message recipient through a server; and

c) said server receives said vector IV3 and said response AR from said recipient, and carries out steps i through k to authenticate said recipient.

10. A method as described in claim 6 where H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

11. A method as described in claim 10 where said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system.

12. A method as described in claim 11 where said encryption algorithm is an RC4 algorithm.

13. A method for responding to an authentication challenge, said method comprising the steps of:

a) receiving initialization vectors IV1 and IV2;

b) generating an authentication response key as H(IV1 | P), where P is a password received from a sender;

c) generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

d) generating a third random number as a third initialization vector IV3;

e) generating an authentication response key ARK as H(IV2 | IV3 | AS);

f) generating an authentication response AR as E(ACNST2, ARK); and

g) sending (IV3, AR) to said sender.

14. A method as described in claim 13 where:

a) steps a through f are carried out by a message recipient;

b) said message recipient sends said vector IV3 and said response AR to a server; and

c) said server receives said vector IV3 and said response AR from said recipient, and authenticates said recipient.

15. A method as described in claim 13 where H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

16. A method as described in claim 15 where said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system.

17. A method as described in claim 16 where said encryption algorithm is an RC4 algorithm.

18. A method for receiving an encrypted message, said method comprising the steps of:

a) receiving (IV4, ENC), where ENC = E(M | H(M), PK), M is said message, and E is a predetermined encryption algorithm;

b) generating PK as H(IV4 | P), where P is a password received from a sender of said message over a secure channel;

c) generating D(ENC, PK) = (M | H(M)), where D is a symmetric key decryption algorithm corresponding to E;

d) calculating H(M) from said value of M generated in step c; and

e) accepting said generated value of M only if said calculated value of H(M) equals said value of H(M) generated in step c.

19. A method as described in claim 18 where H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

20. A method as described in claim 19 where said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system.

21. A method as described in claim 16 where said encryption algorithm is an RC4 algorithm.

22. A method as described in claim 18 where said initialization vector IV4 and said encryption ENC are received from said sender through a server.

23. A method for secure communication of a message to a message recipient, said method comprising the steps of:

a) sending message data encrypted with a symmetric key algorithm, a private key for said encryption algorithm being generated by hashing first data, said first data including a password; where

b) said first data is hashed with an encryption algorithm defined hash algorithm using said encryption algorithm.

24. A method as described in claim 23 further comprising the steps of:

a) authenticating a message recipient by the exchange of second data encrypted with said encryption algorithm, an authentication key for said encryption algorithm being generated by hashing third data, said third data including a password; where

b) said third data is hashed with an encryption algorithm defined hash algorithm using said encryption algorithm.

25. A method as described in claim 24 where said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system.

26. A method as described in claim 24 where said encryption algorithm is an RC4 algorithm.

27. A sender data processing system for use in a system for authenticating a message recipient, said sender data processing system being programmed to:

a) generate a password P;

b) send said password P to said message recipient over a first, secure channel;

c) generate a first random number as a first initialization vector IV1;

d) generating H(IV1 | P) as an authentication key AK;

e) generate an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm; and

f) send said vector IV1 to said message recipient over a second channel; where

g) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

28. A server data processing system for use in a system for authenticating a message recipient, said server data processing system being programmed to:

a) receive an authentication string AS and a first initialization vector IV1 from a sender;

b) generate a second random number as a second initialization vector IV2;

c) send said vectors IV1 and IV2 to a message recipient;

d) receive a third random number as a third initialization vector IV3 and an authentication response AR from said recipient over said second channel;

e) make a predetermined selection of an authentication response key ARK as H(IV2 | IV3 | AS);

f) generate a decryption D(AR, ARK), where D is a symmetric decryption algorithm corresponding to E; and

g) authenticating said message recipient only if D(AR, ARK) = ACNST2, where ACNST2 is a second predetermined constant; where

h) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

29. A message recipient data processing system for use in a system for authenticating a message recipient, said message recipient data processing system being programmed to:

a) receive initialization vectors IV1 and IV2;

b) generating an authentication key AK as H(IV1 | P), where P is a password received from a sender;

c) generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

d) generate a third random number as a third initialization vector IV3;

e) generating an authentication response key ARK as H(IV2 | IV3 | AS);

f) generate an authentication response AR as E(ACNST2, ARK); and

g) send (IV3, AR) to said sender; where

h) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

30. A sender data processing system for use in a system for secure communication of a message to a message recipient, said sender data processing system being programmed to:

a) generate a random number as an initialization vector IV4;

b) generate a private key PK as H(IV4 | P), where P is a password known to a message recipient;

c) generate an encryption ENC = E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm; and

d) send (IV4, ENC) to said message recipient; where

e) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

31. A message recipient data processing system for use in a system for secure communication of a message to a message recipient, said message recipient data processing system being programmed to:

a) receive (IV4, ENC), where ENC = E(M | H(M), PK), M is said message, and E is a predetermined encryption algorithm;

b) generating PK as H(IV4 | P), where P is a password received from a sender of said message over a secure channel;

c) generate D(ENC, PK) = (M | H(M)), where D is a symmetric key decryption algorithm corresponding to E;

d) calculate H(M) from said value of M generated in step c; and

e) accept said generated value of M only if said calculated value of H(M) equals said value of H(M) generated in step c; where

f) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

32. A computer-readable medium carrying one or more sequences of one or more instructions for controlling a sender data processing system to:

a) generate a password P;

b) send said password P to said message recipient over a first, secure channel;

c) generate a first random number as a first initialization vector IV1;

d) generating H(IV1 | P) as an authentication key AK;

e) generate an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm; and

f) send said vector IV1 to said message recipient over a second channel; where

g) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

33. A computer-readable medium carrying one or more sequences of one or more instructions for controlling a server data processing system to:

a) receive an authentication string AS and a first initialization vector IV1 from a sender;

b) generate a second random number as a second initialization vector IV2;

c) send said vectors IV1 and IV2 to a message recipient;

d) receive a third random number as a third initialization vector IV3 and an authentication response AR from said recipient over said second channel;

e) make a predetermined selection of an authentication response key ARK as H(IV2 | IV3 | AS);

f) generate a decryption D(AR, ARK), where D is a symmetric decryption algorithm corresponding to E; and

g) authenticating said message recipient only if D(AR, ARK) = ACNST2, where ACNST2 is a second predetermined constant; where

h) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

34. A computer-readable medium carrying one or more sequences of one or more instructions for controlling a message recipient data processing system to:

a) receive initialization vectors IV1 and IV2;

b) generate an authentication key AR as H(IV1 | P), where P is a password received from a sender;

c) generate an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

d) generate a third random number as a third initialization vector IV3;

e) make a predetermined selection of an authentication response key ARK as H(IV2 | IV3 | AS);

f) generate an authentication response AR as E(ACNST2, ARK); and

g) send (IV3, AR) to said sender; where

h) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

35. A computer-readable medium carrying one or more sequences of one or more instructions for controlling a sender data processing system to:

a) generate a random number as an initialization vector IV4;

b) generate a private key PK as H(IV4 | P), where P is a password known to a message recipient;

c) generate an encryption ENC = E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm; and

d) send (IV4, ENC) to said message recipient; where

e) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

36. A computer-readable medium carrying one or more sequences of one or more instructions for controlling a message recipient data processing system to:

a) receive initialization vectors IV1 and IV2;

b) generate an authentication key AR as H(IV1 | P), where P is a password received from a sender;

c) generate an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

d) generate a third random number as a third initialization vector IV3;

e) make a predetermined selection of an authentication response key ARK as H(IV2 | IV3 | AS);

f) generate an authentication response AR as E(ACNST2, ARK); and

g) send (IV3, AR) to said sender; where

h) H is an encryption algorithm defined hash algorithm using said encryption algorithm E.